

# Skew cyclic codes over $\mathbb{F}_q + v\mathbb{F}_q + v^2\mathbb{F}_q$ \*

Minjia SHI, Ting YAO

(School of Mathematical Sciences of Anhui University. Anhui, China.)

Adel Alahmadi, Patrick Solé

(Department of Mathematics of King Abdulaziz University. Jeddah, Saudi Arabia)

**Abstract:** In this article, we study skew cyclic codes over ring  $R = \mathbb{F}_q + v\mathbb{F}_q + v^2\mathbb{F}_q$ , where  $q = p^m$ ,  $p$  is an odd prime and  $v^3 = v$ . We describe generator polynomials of skew cyclic codes over this ring and investigate the structural properties of skew cyclic codes over  $R$  by a decomposition theorem. We also describe the generator polynomials of the duals of skew cyclic codes. Moreover, the idempotent generators of skew cyclic codes over  $\mathbb{F}_q$  and  $R$  are considered.

**Key words:** Linear codes; Dual codes; Skew cyclic codes; Generator polynomial; Gray map

**MSC (2010) :** Primary 94B05; Secondary 94B60.

## 1 Introduction

Codes over finite rings have been studied since the early 1970s, because of their rich structure, linear codes are the most frequent in coding theory. While different approaches have been applied to produce certain types of codes with good parameters and properties. In [8], Hammons et al. showed that some important binary nonlinear codes can be obtained from cyclic codes over  $\mathbb{Z}_4$  through the Gray map. Recently, in [2], D. Boucher et al. introduced the class of  $\theta$ -cyclic (skew cyclic) codes that generalizes the concept of cyclic codes over non-commutative polynomial rings, called a skew polynomial ring, to construct these types of codes.

In [2], D. Boucher et al. gave skew cyclic codes defined by using the skew polynomial ring

---

\***Foundation item:** Supported by NNSF of China (61202068), Talents youth Fund of Anhui Province Universities (2012SQRL020ZD). **Biography:**SHI Min-jia (corresponding author), male, born in 1980, PhD. Research field: coding theory and cryptography. E-mail: smjwcl.good@163.com. **This manuscript was finished on 2014/12/01, now it was accepted for publication by a magazine, which was submitted on 2015/02/03.**

with an automorphism  $\theta$  over the finite field with  $q$  elements. The polynomial ring is denoted by  $\mathbb{F}_q[x, \theta]$ , where the addition is the usual polynomial addition and the multiplication is defined by the rule  $xa = \theta(a)x, (a \in \mathbb{F}_q)$  in [9] which means the finite field elements are not commutative with the indeterminate  $x$ . In [3], D. Boucher and F. Ulmer showed that the dual of a  $\theta$ -cyclic code is still a  $\theta$ -cyclic code. I. Siap et al. [10] gave the structure of skew cyclic codes of arbitrary length. J. Gao in [6] studied skew cyclic codes over  $\mathbb{F}_p + v\mathbb{F}_p$ . In [7], F. Gursoy et al. presented the construction of skew cyclic codes over  $\mathbb{F}_q + v\mathbb{F}_q$  for different automorphisms. Moreover, T. Abualrub et al. [1] and D. Boucher et al. [4] studied skew quasi-cyclic codes and skew constacyclic codes, respectively.

In this paper, we study skew cyclic codes defined by the skew polynomial ring with coefficients over ring  $R = \mathbb{F}_q + v\mathbb{F}_q + v^2\mathbb{F}_q$ , where  $q = p^m$ ,  $p$  is an odd prime and  $v^3 = v$ . In our work, we consider the automorphisms

$$\begin{aligned}\theta_i : \mathbb{F}_q + v\mathbb{F}_q + v^2\mathbb{F}_q &\rightarrow \mathbb{F}_q + v\mathbb{F}_q + v^2\mathbb{F}_q \\ a + bv + cv^2 &\mapsto a^{p^i} + vb^{p^i} + v^2c^{p^i}.\end{aligned}$$

Denote the skew polynomial ring as  $R[x, \theta_i]$ , where the addition is the usual polynomial addition and the multiplication is defined by the rule  $xa = \theta_i(a)x, (a \in R)$ .

The rest of the paper is organized as follows: Section 2 gives a Gray map from  $R$  to  $\mathbb{F}_q^3$ . In Section 3, we mainly describe the basic properties of linear codes over  $R$  and their structures. In Section 4, we describe the generator polynomials of skew cyclic codes and the duals of skew cyclic codes. We prove that every skew cyclic code over  $R$  is principally generated and give the idempotent generators of  $\mathbb{F}_q$  and  $\mathbb{F}_q + v\mathbb{F}_q + v^2\mathbb{F}_q$ .

## 2 Preliminary

Let  $R = \mathbb{F}_q + v\mathbb{F}_q + v^2\mathbb{F}_q$ , where  $q = p^m$ ,  $p$  is an odd prime and  $v^3 = v$ . Clearly,  $R \cong \mathbb{F}_q[v]/(v^3 - v)$ .  $R$  is a commutative ring with identity and characteristic  $p$ . For any element  $r$  of  $R$ ,  $r$  can be expressed uniquely as  $r = a + bv + cv^2$ , where  $a, b, c \in \mathbb{F}_q$ . It is easily checked that  $R$  is a Frobenius ring but not local.  $R$  is also principal and has three maximal ideals  $\langle v \rangle, \langle v - 1 \rangle$  and  $\langle v + 1 \rangle$ .

From [5], we have the following definition.

**Definition 2.1** The definition of the Gray map on  $R^n$  as follows

$$\Phi : R^n \rightarrow \mathbb{F}_q^{3n}$$

$$(r_0, r_1, \dots, r_{n-1}) \rightarrow (a_0, a_0 + b_0 + c_0, a_0 - b_0 + c_0, \dots, a_{n-1}, a_{n-1} + b_{n-1} + c_{n-1}, a_{n-1} - b_{n-1} + c_{n-1}),$$

where  $r_i = a_i + b_i v + c_i v^2, i = 0, 1, \dots, n - 1$ .

**Definition 2.2** Let  $r = a + bv + cv^2$  be an element of  $R$ , then the Lee weight of  $r$  is defined as

$$\omega_L(r) = \omega_H(a, a + b + c, a - b + c),$$

where the symbol  $\omega_H(v)$  denotes the Hamming weight of  $v$  over  $\mathbb{F}_q$ .

### 3 Linear codes over $R$

In this section, we generalize the structure and properties from [5] to codes over  $R$ . Hence the proofs of many of the theorems will be omitted.

**Lemma 3.1** ([5, Lemma 1]) The Gray map  $\Phi$  is a distance-preserving map from  $(R^n, \text{Lee distance})$  to  $(\mathbb{F}_q^{3n}, \text{Hamming distance})$  and it is also  $\mathbb{F}_q$ -linear.

According to the definition of the Gray map  $\Phi$  and Lemma 3.1, we have the following lemma.

**Lemma 3.2** Let  $C$  be a linear code of length  $n$  over  $R$  with rank  $k$  and minimum Lee distance  $d$ , then  $\Phi(C)$  is a  $[3n, k, d]$  linear code over  $\mathbb{F}_q$ .

**Proof** From Lemma 3.1, we see that  $\Phi(C)$  is a  $\mathbb{F}_q$ -linear code. From the definition of the Gray map. We can easily obtain that  $\Phi(C)$  has dimension  $k$  and length  $3n$  since  $\Phi$  is a bijective map from  $R^n$  to  $\mathbb{F}_q^{3n}$ . Moreover, since Gray map  $\Phi$  is a distance-preserving map, so  $\Phi(C)$  has the same minimum distance  $d$ .

Let  $C$  be a linear code over  $R$ . The dual of  $C$  consists of all vectors of  $R^n$  which are orthogonal to every codeword in  $C$ . A code  $C$  is said to be self-dual (resp. self-orthogonal) if  $C = C^\perp$  (resp.  $C \subseteq C^\perp$ ). Now, in light of Ref.[5], we give the following theorem.

**Theorem 3.1** ([5, Theorem 1]) Let  $C$  be a linear code over  $R$ , then  $\Phi(C)^\perp = \Phi(C^\perp)$ . Moreover, if  $C$  is self-dual, so is  $\Phi(C)$  over  $\mathbb{F}_q$ .

By the Chinese Remainder Theorem, we have

$$\begin{aligned} R &= (1 - v^2)R \oplus (2^{-1}v + 2^{-1}v^2)R \oplus (-2^{-1}v + 2^{-1}v^2)R \\ &= (1 - v^2)\mathbb{F}_q \oplus (2^{-1}v + 2^{-1}v^2)\mathbb{F}_q \oplus (-2^{-1}v + 2^{-1}v^2)\mathbb{F}_q. \end{aligned}$$

For the sake of convenience, we denote by  $\eta_1, \eta_2, \eta_3$  respectively the following elements of  $R$ .

$$\eta_1 = 1 - v^2, \eta_2 = 2^{-1}v + 2^{-1}v^2, \eta_3 = -2^{-1}v + 2^{-1}v^2.$$

Note that  $\eta_1, \eta_2$ , and  $\eta_3$  are mutually orthogonal idempotents over  $R$  and  $\eta_1 + \eta_2 + \eta_3 = 1$ .

Let  $C$  be a linear code of length  $n$  over  $R$ . Define

$$\begin{aligned} C_1 &= \{x \in \mathbb{F}_q^n \mid \exists y, z \in \mathbb{F}_q^n, \eta_1 x + \eta_2 y + \eta_3 z \in C\}, \\ C_2 &= \{y \in \mathbb{F}_q^n \mid \exists x, z \in \mathbb{F}_q^n, \eta_1 x + \eta_2 y + \eta_3 z \in C\}, \\ C_3 &= \{z \in \mathbb{F}_q^n \mid \exists x, y \in \mathbb{F}_q^n, \eta_1 x + \eta_2 y + \eta_3 z \in C\}. \end{aligned}$$

Then  $C_1, C_2, C_3$  are all linear codes of length  $n$  over  $\mathbb{F}_q$ . Moreover, the code  $C$  of length  $n$  over  $R$  can be uniquely expressed as

$$C = \eta_1 C_1 \oplus \eta_2 C_2 \oplus \eta_3 C_3.$$

Let  $G_1, G_2$  and  $G_3$  be the generator matrices of  $C_1, C_2$  and  $C_3$ , respectively, then

$$G = \begin{pmatrix} \eta_1 G_1 \\ \eta_2 G_2 \\ \eta_3 G_3 \end{pmatrix}$$

is the generator matrix of  $C$ .

According to Definition 2.1, we can easily obtain the following proposition.

**Proposition 3.1** If  $C$  is a linear code of length  $n$  over  $R$  with generator matrix  $G$ , then we have

$$\Phi(G) = \begin{pmatrix} \Phi(\eta_1 G_1) \\ \Phi(\eta_2 G_2) \\ \Phi(\eta_3 G_3) \end{pmatrix} = \begin{pmatrix} G_1 & 0 & 0 \\ 0 & G_2 & 0 \\ 0 & 0 & G_3 \end{pmatrix}.$$

Moreover,  $d_H(\Phi(C)) = \min\{d_H(C_1), d_H(C_2), d_H(C_3)\}$ .

**Theorem 3.2** ([5, Theorem 3]) Let  $C$  be a linear code of length  $n$  over  $R$ , then

$$C^\perp = \eta_1 C_1^\perp \oplus \eta_2 C_2^\perp \oplus \eta_3 C_3^\perp.$$

Moreover,  $C$  is self-dual if and only if  $C_1, C_2$  and  $C_3$  are all self-dual over  $\mathbb{F}_q$ .

## 4 Skew cyclic codes over $R$

In this section, we mainly study skew cyclic codes over  $R$  with automorphism  $\theta_i$  and give the generator polynomials of skew cyclic codes and their dual codes. Let us denote the order of  $\theta_i$ , which is  $t_i = \frac{m}{i}$  for some positive integer. In the commutative case if  $(n, q) = 1$ , then every cyclic code of length  $n$  over  $\mathbb{F}_q$  has a unique idempotent generator. Note that in the skew polynomial ring  $\mathbb{F}_q[x, \theta_i]$ , if  $(n, t_i) = 1$ , then the factorization of  $x^n - 1$  in  $\mathbb{F}_q[x, \theta_i]$  is unique (see [7]). In this part, we also show that a formula for the number of skew cyclic codes of length  $n$  over  $R$  when  $(n, t_i) = 1$ .

We first give the concept of skew cyclic codes over  $R$ .

**Definition 4.1** Let  $R$  be a ring and  $\theta_i$  be an automorphism of  $R$ . A linear code  $C$  of length  $n$  over  $R$  is a skew cyclic code with the property that

$$c = (c_0, c_1, \dots, c_{n-1}) \in C \Rightarrow \sigma(c) = (\theta_i(c_{n-1}), \theta_i(c_0), \dots, \theta_i(c_{n-2})) \in C,$$

where  $\sigma(c)$  is a skew cyclic shift of  $c$ .

In polynomial representation, the codewords  $(c_0, c_1, \dots, c_{n-1})$  of a skew cyclic code are coefficient tuples of elements  $c_{n-1}x^{n-1} + \dots + c_1x + c_0 \in R[x, \theta_i]/(x^n - 1)$  which are left multiple of one element  $G \in R[x, \theta_i]/(x^n - 1)$  (the generator polynomial). The multiplication is defined by the basic rule  $(ax^i)(bx^j) = a\theta^i(b)x^{i+j}$ , but this multiplication is not commutative.

**Lemma 4.1** ([10]) A linear code of length  $n$  over  $\mathbb{F}_q$  is a skew cyclic code if and only if it is a left  $\mathbb{F}_q[x, \theta]$ -submodule of  $\mathbb{F}_q[x, \theta]/(x^n - 1)$ . Moreover, if  $C$  is a left submodule of  $\mathbb{F}_q[x, \theta]/(x^n - 1)$ , then  $C$  is generated by a monic polynomial  $g(x)$  which is a right divisor of  $x^n - 1$  in  $\mathbb{F}_q[x, \theta]$ .

**Theorem 4.1** Let  $C$  be a linear code over  $R$  of length  $n$  and  $C = \eta_1 C_1 \oplus \eta_2 C_2 \oplus \eta_3 C_3$ , where  $C_1, C_2$  and  $C_3$  are codes over  $\mathbb{F}_q$  of length  $n$ , then  $C$  is a skew cyclic code with respect to the automorphism  $\theta_i$  if and only if  $C_1, C_2$  and  $C_3$  are skew cyclic codes over  $\mathbb{F}_q$  with respect to the automorphism  $\theta_i$ .

**Proof** Let  $(a_0, a_1, \dots, a_{n-1}) \in C_1, (b_0, b_1, \dots, b_{n-1}) \in C_2$  and  $(c_0, c_1, \dots, c_{n-1}) \in C_3$ . Assume that  $r_i = \eta_1 a_i + \eta_2 b_i + \eta_3 c_i$  for  $i = 0, 1, \dots, n-1$ , then the vector  $(r_0, r_1, \dots, r_{n-1}) \in C$ . If  $C$  is a skew cyclic code then  $(\theta_i(r_{n-1}), \theta_i(r_0), \dots, \theta_i(r_{n-2})) \in C$ , note that  $\sigma(r) = (\theta_i(r_{n-1}), \theta_i(r_0), \dots, \theta_i(r_{n-2})) = \eta_1(a_{n-1}^{p^i}, a_0^{p^i}, \dots, a_{n-2}^{p^i}) + \eta_2(b_{n-1}^{p^i}, b_0^{p^i}, \dots, b_{n-2}^{p^i}) + \eta_3(c_{n-1}^{p^i}, c_0^{p^i}, \dots, c_{n-2}^{p^i})$ . Hence,  $(\theta_i(a_{n-1}), \theta_i(a_0), \dots, \theta_i(a_{n-2})) = (a_{n-1}^{p^i}, a_0^{p^i}, \dots, a_{n-2}^{p^i}) \in C_1, (\theta_i(b_{n-1}), \theta_i(b_0), \dots, \theta_i(b_{n-2})) \in C_2, (\theta_i(c_{n-1}), \theta_i(c_0), \dots, \theta_i(c_{n-2})) \in C_3$ , which implies that  $C_1, C_2, C_3$  are skew cyclic codes over  $\mathbb{F}_q$ .

On the other hand, suppose that  $C_1, C_2$  and  $C_3$  are all skew cyclic codes over  $\mathbb{F}_q$  and  $(r_0, r_1, \dots, r_{n-1}) \in C$ , where  $r_i = \eta_1 a_i + \eta_2 b_i + \eta_3 c_i$  for  $i = 0, 1, \dots, n-1$ , then  $(a_0, a_1, \dots, a_{n-1}) \in C_1, (b_0, b_1, \dots, b_{n-1}) \in C_2$  and  $(c_0, c_1, \dots, c_{n-1}) \in C_3$ . Note that  $\sigma(r) = (\theta_i(r_{n-1}), \theta_i(r_0), \dots, \theta_i(r_{n-2})) = \eta_1(a_{n-1}^{p^i}, a_0^{p^i}, \dots, a_{n-2}^{p^i}) + \eta_2(b_{n-1}^{p^i}, b_0^{p^i}, \dots, b_{n-2}^{p^i}) + \eta_3(c_{n-1}^{p^i}, c_0^{p^i}, \dots, c_{n-2}^{p^i}) = \eta_1(\theta_i(a_{n-1}), \theta_i(a_0), \dots, \theta_i(a_{n-2})) + \eta_2(\theta_i(b_{n-1}), \theta_i(b_0), \dots, \theta_i(b_{n-2})) + \eta_3(\theta_i(c_{n-1}), \theta_i(c_0), \dots, \theta_i(c_{n-2})) \in \eta_1 C_1 \oplus \eta_2 C_2 \oplus \eta_3 C_3 = C$ , so  $C$  is a skew cyclic code over  $R$ .

From Theorem 4.1, we can easily prove the following corollary.

**Corollary 4.1** If  $C$  be a skew cyclic code over  $R$ , then the dual code  $C^\perp$  is also skew cyclic.

**Proof** By Theorem 3.2, we have  $C^\perp = \eta_1 C_1^\perp \oplus \eta_2 C_2^\perp \oplus \eta_3 C_3^\perp$ . According to [3, Corollary 18], we know that the dual code of every skew cyclic code over  $\mathbb{F}_q$  is also skew cyclic. Hence the dual code  $C^\perp$  is a skew cyclic code from Theorem 4.1.

**Definition 4.2** Let  $\mathcal{C}$  be a linear code of length  $n$  over  $\mathbb{F}_q$  and  $c = (c_0, c_1, \dots, c_{n-1}) = (c^1 | c^2 | \dots | c^l)$  be a codeword in  $\mathcal{C}$  divided into  $l$  equal parts of length  $m$  where  $n = ml$ . If  $\varphi_l = (\sigma(c^1) | \sigma(c^2) | \dots | \sigma(c^l)) \in \mathcal{C}$ , where  $\varphi$  is the usual cyclic shift of  $C$ , then the linear code  $C$  which is permutation equivalent to  $\mathcal{C}$  is called a skew quasi-cyclic code of index  $l$ .

The next corollary follows from the definition of quasi-cyclic codes.

**Corollary 4.2** If  $C$  is a skew cyclic code of length  $n$  over  $R$ , then  $\Phi(C)$  is a skew 3-quasi cyclic code of length  $3n$  over  $\mathbb{F}_q$ .

**Proof** The result follows from the Definition 4.2 and Definition 2.1.

We are now ready to consider the generator polynomial of a skew cyclic code with length  $n$  over  $R$ .

**Theorem 4.2** Let  $C = \eta_1 C_1 \oplus \eta_2 C_2 \oplus \eta_3 C_3$  be a skew cyclic code of length  $n$  over  $R$  and assume that  $g_1(x), g_2(x)$  and  $g_3(x)$  are generator polynomials of  $C_1, C_2$  and  $C_3$ , respectively, then  $C = \langle \eta_1 g_1(x), \eta_2 g_2(x), \eta_3 g_3(x) \rangle$  and  $|C| = q^{3n - \sum_{i=1}^3 \deg(g_i(x))}$ .

**Proof** Since  $C_1 = \langle g_1(x) \rangle, C_2 = \langle g_2(x) \rangle, C_3 = \langle g_3(x) \rangle$ ,  $|C_i| = q^{n - \deg(g_i(x))}, i = 1, 2, 3$ , and  $C = \eta_1 C_1 \oplus \eta_2 C_2 \oplus \eta_3 C_3$ , then

$$C = \{c(x) = \eta_1 k_1(x)g_1(x) + \eta_2 k_2(x)g_2(x) + \eta_3 k_3(x)g_3(x) \mid k_1(x), k_2(x), k_3(x) \in F_q[x, \theta_i]\},$$

so,  $C \subseteq \langle \eta_1 g_1(x), \eta_2 g_2(x), \eta_3 g_3(x) \rangle$ .

Conversely, let us take  $\eta_1 l_1(x)g_1(x) + \eta_2 l_2(x)g_2(x) + \eta_3 l_3(x)g_3(x) \in \langle \eta_1 g_1(x), \eta_2 g_2(x), \eta_3 g_3(x) \rangle$ , where  $l_1(x), l_2(x), l_3(x) \in R[x, \theta_i]/(x^n - 1)$ , then  $\eta_1 l_1(x) = \eta_1 k_1(x), \eta_2 l_2(x) = \eta_2 k_2(x), \eta_3 l_3(x) = \eta_3 k_3(x)$  for some  $k_1(x), k_2(x), k_3(x) \in F_q[x, \theta_i]$ . Hence  $\langle \eta_1 g_1(x), \eta_2 g_2(x), \eta_3 g_3(x) \rangle \subseteq C$ . Therefore,  $C = \langle \eta_1 g_1(x), \eta_2 g_2(x), \eta_3 g_3(x) \rangle$ . Since  $|C| = |C_1||C_2||C_3|$ , then we have  $|C| = q^{3n - \sum_{i=1}^3 \deg(g_i(x))}$ .

**Theorem 4.3** Let  $C_1, C_2$  and  $C_3$  be skew cyclic codes over  $\mathbb{F}_q$  and  $g_1, g_2, g_3$  be the monic generator polynomials of  $C_1, C_2$  and  $C_3$ , respectively. Suppose that  $C = \eta_1 C_1 \oplus \eta_2 C_2 \oplus \eta_3 C_3$ , then there exists a unique polynomial  $g(x) \in R[x, \theta_i]$  such that  $C = \langle g(x) \rangle$  and  $g(x)$  is a right divisor of  $x^n - 1$ , where  $g(x) = \eta_1 g_1(x) + \eta_2 g_2(x) + \eta_3 g_3(x)$ .

**Proof** Let  $g(x) = \eta_1 g_1(x) + \eta_2 g_2(x) + \eta_3 g_3(x)$ , then it is easy to verify that  $\langle g(x) \rangle \subseteq C$ . On the other hand  $\eta_1 g_1(x) = \eta_1 g(x), \eta_2 g_2(x) = \eta_2 g(x), \eta_3 g_3(x) = \eta_3 g(x)$ , which implies that  $C \subseteq \langle g(x) \rangle$ . Thus  $C = \langle g(x) \rangle$ .

Since  $g_1(x), g_2(x), g_3(x)$  are monic right divisors of  $x^n - 1$  in  $\mathbb{F}_q[x, \theta_i]$ , then there are  $h_1(x), h_2(x), h_3(x)$  in  $\mathbb{F}_q[x, \theta_i]/(x^n - 1)$  such that  $x^n - 1 = h_1(x)g_1(x) = h_2(x)g_2(x) =$

$h_3(x)g_3(x)$ . Thus

$$\begin{aligned}
[\eta_1 h_1(x) + \eta_2 h_2(x) + \eta_3 h_3(x)]g(x) &= [\eta_1 h_1(x) + \eta_2 h_2(x) + \eta_3 h_3(x)] \cdot \\
&\quad [\eta_1 g_1(x) + \eta_2 g_2(x) + \eta_3 g_3(x)] \\
&= [\eta_1 h_1(x)g_1(x) + \eta_2 h_2(x)g_2(x) + \eta_3 h_3(x)g_3(x)] \\
&= [\eta_1(x^n - 1) + \eta_2(x^n - 1) + \eta_3(x^n - 1)] \\
&= x^n - 1.
\end{aligned}$$

Hence  $g(x)$  is a right divisor of  $x^n - 1$ .

The following corollary follows easily.

**Corollary 4.3** Every left submodule of  $R[x, \theta_i]/(x^n - 1)$  is principally generated.

Let  $g(x) = \sum_{i=0}^r g_i x^i$  and  $h(x) = \sum_{i=0}^{n-r} h_i x^i$  be polynomials in  $\mathbb{F}_q[x, \theta_i]$  such that  $x^n - 1 = h(x)g(x)$  and  $C$  be the skew cyclic code generated by  $g(x)$  in  $\mathbb{F}_q[x, \theta_i]/(x^n - 1)$ . Then the dual code of  $C$  is a skew cyclic code generated by the polynomial  $\tilde{h}(x) = h_{n-r} + \theta_i(h_{n-r-1})x + \dots + \theta_i^{n-r}(h_0)x^{n-r}$  ([3] Corollary 18).

**Corollary 4.4** Let  $C_1, C_2, C_3$  be skew cyclic codes over  $\mathbb{F}_q$  and  $g_1, g_2, g_3$  be their generator polynomials such that  $x^n - 1 = h_1 g_1, x^n - 1 = h_2 g_2, x^n - 1 = h_3 g_3$  in  $\mathbb{F}_q[x, \theta_i]$ . If  $C = \eta_1 C_1 \oplus \eta_2 C_2 \oplus \eta_3 C_3$ , then  $C^\perp = \langle h(x) \rangle$  where  $h(x) = \eta_1 \tilde{h}_1(x) + \eta_2 \tilde{h}_2(x) + \eta_3 \tilde{h}_3(x)$  and  $|C^\perp| = q^{\sum_{i=1}^3 \deg(g_i(x))}$ .

**Proof** By Theorem 3.2, we have  $C^\perp = \eta_1 C_1^\perp \oplus \eta_2 C_2^\perp \oplus \eta_3 C_3^\perp$ . Since  $C_1^\perp = \langle \tilde{h}_1(x) \rangle, C_2^\perp = \langle \tilde{h}_2(x) \rangle$ , and  $C_3^\perp = \langle \tilde{h}_3(x) \rangle$ , we conclude by Theorem 4.3 that  $C^\perp = \langle h(x) \rangle$ .

In the following section, we denote the order of  $\theta_i$  is  $t_i = \frac{m}{i}$  for some positive integer and  $(n, t_i) = 1$ .

**Lemma 4.2** ([7, Lemma 2]) Let  $g(x) \in \mathbb{F}_q[x, \theta_i]$  be a monic right divisor of  $x^n - 1$ . If  $(n, t_i) = 1$ , then  $g(x) \in \mathbb{F}_{p^i}[x]$ .

The proof of Theorem 4.4 is similar to that of [7, Theorem 6], so we omit the proof here.

**Theorem 4.4** Let  $g(x) \in \mathbb{F}_q[x, \theta_i]$  be a monic right divisor of  $x^n - 1$  and  $C = \langle g(x) \rangle$ . If  $(n, q) = 1$  and  $(n, t_i) = 1$ , then there exists an idempotent polynomial  $e(x) \in \mathbb{F}_q[x, \theta_i]/(x^n - 1)$  such  $C = \langle e(x) \rangle$ .

From Theorem 4.3 and Theorem 4.4, we have the following corollary.

**Corollary 4.5** Let  $C = \eta_1 C_1 \oplus \eta_2 C_2 \oplus \eta_3 C_3$  be a skew cyclic code of length  $n$  over  $R$  and  $(n, q) = 1, (n, t_i) = 1$ , then  $C_i$  has the idempotent generator  $e_i(x), i = 1, 2, 3$ . Moreover,  $e(x) = \eta_1 e_1(x) \oplus \eta_2 e_2(x) \oplus \eta_3 e_3(x)$  is an idempotent generator of  $C$ , i.e  $C = \langle e(x) \rangle$ .

Gao in [6] showed that a skew cyclic code is equivalent to a cyclic code of length  $n$  over  $\mathbb{F}_p + v\mathbb{F}_p$  with some condition, and gave the enumeration of distinct skew cyclic codes of length  $n$  over  $\mathbb{F}_p + v\mathbb{F}_p$ . From [6], we also give the number of the skew cyclic code of

arbitrary length  $n$  over  $R$ .

**Theorem 4.5** Let  $(n, t_i) = 1$  and  $x^n - 1 = \prod_{i=1}^r p_i^{s_i}(x)$  where  $p_i(x) \in \mathbb{F}_q[x, \theta_i]$  is irreducible. Then the number of skew cyclic codes of length  $n$  over  $R$  is  $\prod_{i=1}^r (s_i + 1)^3$ .

**Proof** By Lemma 4.2, if  $(n, t_i) = 1$ , then  $p_i(x) \in \mathbb{F}_q[x]$ . Hence the number of skew cyclic codes of length  $n$  over  $\mathbb{F}_q$  is  $\prod_{i=1}^r (s_i + 1)$ . By the decomposition theorem, then the number of skew cyclic codes of length  $n$  over  $R$  is  $\prod_{i=1}^r (s_i + 1)^3$ .

## 5 Conclusion

In this article, we investigate skew cyclic codes over  $R = \mathbb{F}_q + v\mathbb{F}_q + v^2\mathbb{F}_q$ , where  $q = p^m$ ,  $p$  is a odd prim, and  $v^3 = v$ . We give the number of skew cyclic codes of length  $n$  over  $\mathbb{F}_q$  and  $\mathbb{F}_q + v\mathbb{F}_q + v^2\mathbb{F}_q$  under certain conditions. We also describe the generator polynomials of skew cyclic codes over the field  $\mathbb{F}_q$  and  $\mathbb{F}_q + v\mathbb{F}_q + v^2\mathbb{F}_q$  and investigate the structural properties of skew cyclic codes over  $R$  by a decomposition theorem and also show their idempotent generators.

## References

- [1] T. Abualrub, A. Ghrayeb, N. Aydin and I. Siap. On the construction of skew quasi-cyclic codes. IEEE T rans. Inform. Theory, 56(2010), 2080-2090.
- [2] D. Boucher, W. Geiselmann and F. Ulmer. Skew cyclic codes. Appl. Algebra Eng. Comm., 18(2007), 379-389.
- [3] D. Boucher and F. Ulmer. Coding with skew polynomial ring. J. Symb. Comput., 44(2009), 1644-1656.
- [4] D. Boucher, P. Solé and F. Ulmer. Skew constacyclic codes over Galois rings. Adv. Math. Commun., 2(2008), 273-292.
- [5] J. Gao. Some results on linear codes over  $\mathbb{F}_p + u\mathbb{F}_p + u^2\mathbb{F}_p$ . J. Appl. Math. Comput, to appear(2014).
- [6] J. Gao. Skew cyclic codes over  $\mathbb{F}_p + v\mathbb{F}_p$ . J. Appl. Math. Inform. 31(2013), 337-342.
- [7] F. Gursoy, I. Siap and B. Yildiz. Construction of skew cyclic codes over  $\mathbb{F}_q + v\mathbb{F}_q$ . Advances in Mathematics of Communications, 8(2014), 313-322.
- [8] A. R. Hammons Jr., P. V. Kumar, A. R. Calderbank, N. J. A. Sloane and P. Solé. The  $\mathbb{Z}_4$ -linearity of Kerdock, Preparata, Coethals, and related codes. IEEE Trans. Inform. Theory, 40(1994), 301-319.
- [9] B. R. McDonald. Finite Rings with Identity. Marcel Dekker Inc., New York, 1974.



- [10] I. Siap, T. Abualrub, N. Ayclin and P, Seneviratne. Skew cyclic codes of arbitrary length. *Int. Nat. Sci.*, 34(2011), 10-20.